Michel Huissoud, Andreas Jordi

Audit im E-Business

Eine Bestandsaufnahme

Die Revisoren gehören im Wirtschaftsleben eher zu denen, die ihren Blick auf die Vergangenheit richten und im hinteren Mittelfeld spielen. Das verschafft ihnen das angenehme Privileg, einen gewissen zeitlichen Abstand zu gewinnen. Sie können sich somit der Unternehmensentwicklung schrittweise anpassen. Im E-Business gilt dieser «Schonzustand» wahrscheinlich nicht mehr. Man erwartet heute vom Revisor, dass er am Ort des Geschehens präsent ist.

Schwerpunkt der am 26. Juni 2001 gemeinsam von der Treuhand-Kammer und dem ISACA-Verband [1] organisierten Tagung war die Revisionspraxis bei E-Business-Anwendungen. Mit den verschiedenen Referenten [2] wurden konkrete Prüfungserfahrungen analysiert, um die Verfahren, die ermittelten Risiken und die schliesslich an die Kunden abgegebenen Empfehlungen zu verstehen. Die wichtigsten Erkenntnisse dieser Tagung sind Gegenstand dieses Artikels.

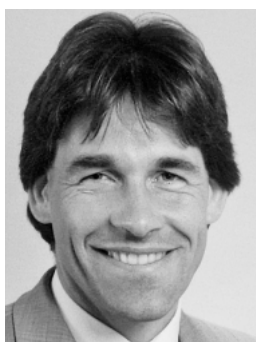
Bei dieser Gelegenheit wurde auch eine vergleichende Studie über Software für E-Shops durchgeführt, um zu erfahren, ob die darin enthaltenen Funktionen den Revisionsansprüchen genügen. Die Ergebnisse dieser Studie werden in einem anderen Artikel in dieser Ausgabe (vgl. S. 1237) besprochen.

1. Wer fühlt sich vom Begriff «Going concern» betroffen?

1.1 Das Jahr 2000: ein Präzedenzfall

1999 war ein bewegtes Jahr. Das hatten wir unseren Kollegen von Übersee zu verdanken. Alles drehte sich darum herauszufinden, ob die für die Jahrtausendwende befürchteten Pannen den Grundsatz der Geschäftskontinuität in Frage stellen würden. Die bisher noch selten in grösserem Umfang zur Anwendung gekommene Revisionsnorm ISA 570 [3] der IFAC [4] (die in Grundsatz zur Abschlussprüfung Nr. 13 der Treuhand-Kammer übernommen wurde) war plötzlich eminent wichtig. Sie rief den externen Revisoren in Erinnerung, dass

- manche Unternehmen von ihren Informatiksystemen äusserst abhängig sind;
- die Fortführung des Geschäfts (going concern) grundsätzlich in Frage gestellt werden müsste, wenn die Informatiksysteme längere Zeit ausfallen;
- in solchen Situationen eventuell die Buchwerte durch Liquidationswerte in der Bilanz ersetzt werden müssen.



Michel Huissoud, lic. iur., CISA, CIA, Mitglied Fachstab für Informatik der Treuhand-Kammer, Vizepräsident ISACA-Schweiz, Vizedirektor bei der Eidgenösischen Finanzkontrolle, Bern

Leider scheinen die Lehren daraus ein Jahr später bereits wieder vergessen zu sein. Die Informatikrevision ist erneut zum Stiefkind der externen Revisoren geworden.

1.2 Wachsende Anfälligkeit und Abhängigkeit der Unternehmen

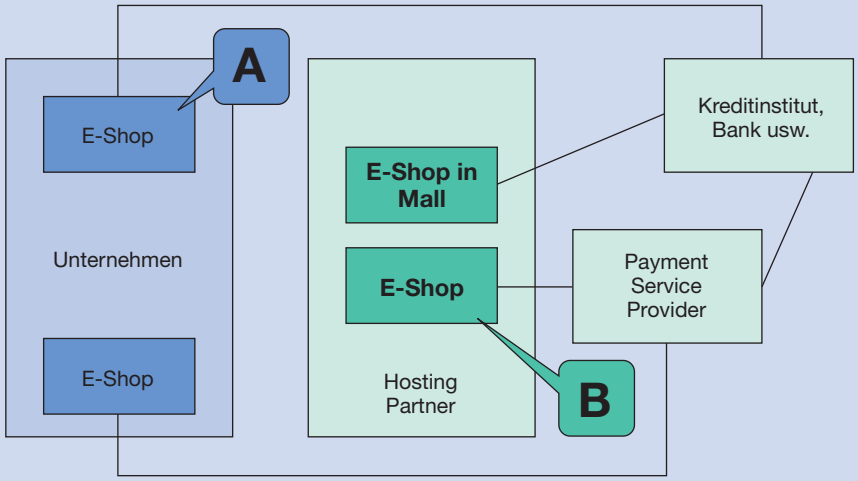
Die Schwierigkeit, die die Beherrschung der verschiedenen Technologien mit sich bringt sowie deren Kosten lassen zahlreiche Unternehmen zum Mittel der Auslagerung (outsourcing) greifen. Das in der *Abbildung 1* abgebildete System der E-Shops sieht im Vergleich zu gewissen E-Banking-Projekten kinderleicht aus. Falls es eines Tages tatsächlich eine elektronische Bank geben sollte, wird diese von ihren Partnern – egal ob im Informatik- oder Finanzbereich – grundsätzlich abhängig sein.

Unter solchen Bedingungen riskiert der externe Revisor eines E-Business-Unternehmens, der dem Grundsatz der Fortführung des Geschäfts zustimmt,

- sich aber nicht um das Vorhandensein geeigneter und wirksamer Katastrophenpläne kümmert,
- keine Erkundigungen über die Solvabilität des Outsourcers einzieht und
- keine Alternativen prüft für den Fall, dass der Outsourcer das Handtuch wirft,

eines Tages für den von unzufriedenen Aktionären oder Dritten erlittenen Schaden haften zu müssen.

Abbildung 1
E-Shop-Varianten



Die schwierige Wahl zwischen der Abhängigkeit gegenüber zwei Partnern (Variante B) und der Unabhängigkeit (Variante A), diese ist allerdings oft mit Mehrkosten oder Unprofessionalität verbunden.

1.3 Und wenn der Markt zusammenbricht?

Eine erneute aufmerksame Lektüre des Grundsatzes Nr. 13 der Treuhand-Kammer wird dem externen Revisor eines E-Business-Unternehmens noch aus einem zweiten Grund aufs Wärmste empfohlen. Darin wird er nämlich aufgefordert, bei seiner Einschätzung der Lage den voraussehbaren externen Faktoren, beispielsweise einem möglichen Marktzusammenbruch, Rechnung zu tragen.

Es wäre interessant – und wahrscheinlich erbaulich – die Bilanzen zu analysieren, die von den heute Konkurs gegangenen Internet-Firmen (Dotcoms) per 31.12.2000 erstellt worden sind. Standen die Aktiven zu entsprechenden Liquidationswerten? Waren die Entwicklungskosten, die über fünf Jahre verteilt werden könnten, im Hinblick auf einen möglichen Marktzusammenbruch abgeschrieben worden? Hatten die Revisoren diese Entwicklung in irgend einer Form berücksichtigt, von der im Frühjahr 2001 alle wussten? Viele Fragen, auf die es wahrscheinlich nie eine Antwort geben wird.

2. Applikationsrevision: keine leichte Sache

2.1 Sitzt ein Pilot am Steuer?

Die gute alte Zeit, als Informatikprojekte in aller Ruhe entwickelt werden konnten, ist vorbei. Heute ist Geschwindigkeit gefragt. Man muss der Konkurrenz zuvorkommen, koste es, was es wolle. Risiken und Einwände der Revisoren zählen kaum. Um dieses Ziel zu erreichen, werden die Projekte in Teilprojekte zerlegt, deren Entwicklung parallel verläuft. Das Problem bei diesem Ansatz ist die extreme Abhängigkeit vom «Piloten», der das Gesamtprojekt steuert. Er muss die Verbindungen zwischen den verschiedenen Partnern und Modulen nicht nur in der Anfangsphase, sondern auch später noch im Griff haben, nämlich dann wenn

- technologische Entwicklungsschübe sich auf ein einzelnes Glied dieser Kette auswirken,
- einer der vorgesehenen Partner zusammenbricht (siehe den Fall der Swisskey),
- die Anwendung in Betrieb genommen wird.

Der Projektleiter muss selbstverständlich ein Spezialist auf dem betreffenden Gebiet sein, ausserdem ein Kommunikationsgenie und ein begnadeter Troubleshooter. Er braucht einen kompetenten Stellvertreter an seiner Seite und muss von der Firma angestellt sein, um zu vermeiden, dass diese in die Abhängigkeit eines externen Beraters gerät.

Letztlich geht es um die Frage, ob jemand die ganze Sache steuert. Die jüngste Vergangenheit hat uns sehr teure Flugzeuge vorgeführt, die sich nie in die Lüfte erheben werden. Sie hat uns auch Flugzeuge gezeigt, die von Mechanikern geflogen werden, Flugzeuge, in denen überhaupt kein Pilot sitzt und Flugzeuge, die angeblich von einem Piloten gesteuert werden, der zwar seine Honorare bezieht, aber gar nicht im Flugzeug sitzt. Am vergangenen 26. Juni sind wir sogar einem Flugzeug begegnet, das aussah, als ob es von seinen Revisoren gesteuert würde.

Andreas Jordi, Ing. HTL, CISA, Prüfungsexperte, Eidgenössische Finanzkontrolle, Bern

2.2 Integration oder Patchwork?

Sobald der Revisor den «grossen Steuermann» ausfindig gemacht hat, wird er zusammen mit diesem prüfen, ob die E-Business-Anwendung gut in die betrieblichen Prozesse und in die Buchhaltungsarchitektur integriert worden ist. Wie schon die Fachmitteilung Nr. 13 der Treuhand-Kammer über den elektronischen Datenaustausch (EDI) emp-

fiehlt, sollte mithilfe einer Prüfspur zum Beispiel der Weg von der Bestellungserfassung bis zum Kundenkonto zurückverfolgt werden können.

Leider muss man in dieser Hinsicht feststellen, dass die marktgängige E-Shop-Software bezüglich der Verbindungen nur sehr begrenzte Möglichkeiten bietet, zum Beispiel mit Programmen für Lagerbewirtschaftung, Produkte- und Kundendatenbank oder Debitorenbuchhaltung.

Hat der Revisor beim Entwerfen der Software keine klaren Vorstellungen geäussert, wird er sich mit ziemlicher Sicherheit mit suboptimalen manuellen Lösungen zufrieden geben müssen. Diese werden so lange brauchbar sein, als die Kunden dem neuen Programm die kalte Schulter zeigen und die Transaktionen ein bescheidenes Volumen nicht übersteigen. Wird die Homepage hingegen von der Kundschaft fleissig besucht, besteht das Risiko, dass die Anwendung bei der Logistik oder Fakturierung Fehler hervorruft und die kommerzielle Entwicklung behindert.

2.3 Der lange Weg vom Kunden bis zur Bilanz der E-Bank

In Ermangelung einer integrierten Lösung wird der Revisor den Prozess nachvollziehen und analysieren müssen. Das beginnt im Falle des E-Banking bei der Aufforderung an den Kunden, Angaben zu seinem Bankauftrag in seinen Computer einzugeben. In diesem Stadium tauchen folgende Fragen auf:

- Ist sich der Kunde über das Wesen der Transaktion, die er gerade tätigt, vollständig im Klaren?
- Führt das System bei den erfassten Daten Plausibilitätskontrollen durch?
- Kann das System garantieren, dass ein Kunde nur zu denjenigen Transaktionen Zugriff hat, zu denen ihn seine Bankverbindung berechtigt?
- Überprüft das System in diesem Stadium bereits die Solvabilität des Kunden?
- Erstellt das System ein Sitzungsprotokoll für den Kunden?
- Ist eine Datenabstimmung zwischen der Erfassung durch den Kunden und dem Eintrag durch das Vorsystem (Frontend) möglich?

Abbildung 2
Der lange Weg zwischen dem Kunde und der Bilanz der E-Bank

Wenn man die Transaktion weiterverfolgt, werden die vom Kunden erfassten Daten anschliessend an das Vorsystem des Unternehmens übermittelt. Der Revisor wird folgende Punkte überprüfen müssen:

- Sind Genauigkeit und Vollständigkeit der übermittelten Daten gewährleistet?
- Wird jede Transaktion, einschliesslich der übertragungsbezogenen Daten (Datum und Uhrzeit, Herkunft, Berechtigung usw.), protokolliert?
- Registriert das System auch die während der Anwendung gültigen Bedingungen (Kurse, Tarife usw.) und leitet es sie an die nächste Anwendung weiter?
- Werden Massnahmen ergriffen, um eine irrtümliche Wiederholung der Transaktion zu vermeiden?
- Findet zwischen dem Vorsystem (Frontend) und der nächsten Anwendung eine Datenabstimmung statt? Wie und wann *(Abbildung 2)*?

Danach folgt die Ausführungsphase der Transaktion, die folgende Fragen aufwirft:

- Wie werden unterbrochene Transaktionen verbucht?
- Wie werden die Transaktionen auf den Bankkonten und auf den Kundenkonten verbucht? Wird jede Transaktion einzeln oder werden die Transaktionen kundenweise verbucht?
- Wie werden die Datenabstimmungen zwischen diesen verschiedenen Verbuchungen sichergestellt?

Dann wird die Transaktion erledigt, ausbezahlt und verbucht. Dabei sind unter anderem folgende Punkte zu überprüfen:

- Wann gilt die Transaktion als abgeschlossen?
- Welche Systeme erhalten eine Meldung?
- Wie reagieren die Systeme, wenn sie keine Meldung erhalten?
- Wann und wie wird der neue Kontostand dem Vorsystem (Frontend) und dem Kunden mitgeteilt?

Bei der Analyse dieses Prozesses dürfen weder der Umgang mit Storni oder Pannen während der Ausführung, noch die Frage eventueller Verzögerungen bei der Ausführung von Bankaufträgen ausgelassen werden.

2.4 Warum nicht einen kurzen Blick auf die Ergonomie werfen?

Eine der Neuheiten im E-Business beruht auf der extremen Flüchtigkeit des Konsumentenverhaltens. Im Gegensatz zu den internen Anwendern einer Informatikanwendung können die Konsumenten ohne weiteres die Firma zugunsten einer benutzerfreundlicheren Oberfläche verlassen. Ein Revisor kennt sich zwar nicht speziell in dieser Art von Prüfungen aus. Man könnte jedoch bspw. einen Informatikprüfer auffordern, Fragen zur Ergonomie einer E-Business-Applikation zu untersuchen, um so festzustellen, ob die Investition auch tatsächlich den gewünschten Erfolg beim potenziellen Kunden haben wird.

3. Sicherheit der Infrastruktur liegt im argen

3.1 Der Kunde ist und bleibt die Schwachstelle im E-Business

Der Szenarien von Computerbetrug oder Datenpiraterie sind viele. Es wird

allgemein anerkannt, dass die grösste Gefahr gegenwärtig darin besteht, dass unter Verwendung der vom Kunden hergestellten Verbindung ohne dessen Wissen ein Angriff gestartet werden kann (z.B. mit einem Passwörter-Sniffer auf seinem PC oder indem die Verbindung mit einem «man-in-the-middle» abgefangen wird).

Ein solcher Angriff ist kaum vermeidbar, denn im allgemeinen entzieht sich die Kundenumgebung der Kontrolle des Unternehmens. Auch wenn es zynisch klingen mag: der Revisor kann nicht viel mehr tun, als zu kontrollieren,

– ob dem Kunden entsprechende Vorsichtsmassnahmen nahegelegt wurden,
– ob die allgemeinen Geschäftsbedingungen oder andere Vertragsklauseln die Haftung des Unternehmens für solche Schadenfälle klar ausschliessen.

Abbildung 3
Beispiel von Piraterie auf einer kommerziellen Homepage (BMW)

Das Risiko besteht zwar tatsächlich, doch es wirft nicht echte Probleme auf, da die Unternehmen äusserst motiviert sind, diese Gefahr gering zu halten.

3.2 Statistisch gesehen lauert die zweitgrösste Betrugsgefahr im Unternehmen selbst

Es gibt keine Informationen, die auf Besonderheiten der E-Business-Applikationen in diesem Bereich hindeuten würden. Sie sind denselben Risiken ausgesetzt wie andere Informatikanwendungen: Anfälligkeit der Betriebssysteme, Unzuverlässigkeit des Informatikpersonals oder der Outsourcer sowie Unsicherheit der lokalen Netzwerke. Wie in den traditionelleren Bereichen erweist sich auch hier eine Informatikprüfung als unabdingbar.

3.3 Die berüchtigten Angriffe von aussen

An dritter Stelle folgen wahrscheinlich die Angriffe externer Urheber. Solche Angriffe sind meist spektakulär (vgl. *Abbildung 3)*. Und sie werden häufig von den Spezialisten für Informatiksicherheit benützt, um Hacking-Aufträge zu verkaufen, die insbesondere Penetrationstests vorsehen.

Solche Angriffe sind nur dann wirklich gefährlich, wenn die Sicherheit der internen Infrastruktur lückenhaft ist. Ein Unternehmen, das seine internen Risiken im Griff hat, braucht externe Angreifer kaum zu fürchten, es sei denn, es sei besonders attraktiv, wie zum Beispiel das Wirtschaftsforum von Davos und seine Homepage.

3.4 Sonderfall der Public Key Infrastructure

In mancherlei Bereichen des E-Business werden heute Verschlüsselungstechniken verwendet: Austausch von chiffrierten Mitteilungen, Schutz des Übertragungskanals durch dessen Verschlüsselung oder aber Verschlüsselung erfasster Daten. Für die Revisoren tut sich hier ein neues Prüfungsfeld auf.

Der Revisor, der damit beauftragt wurde zu prüfen, wie mit diesen Technologien umgegangen wird, muss als erstes kontrollieren, ob ihre Umsetzung den verschiedenen vom Unternehmen im Sicherheitsbereich erlassenen Richtlinien und Weisungen entspricht. Die Certificate Policy und das Certification Practice Statement, die von den Lieferanten dieser Dienstleistungen ausgearbeitet worden sind, enthalten bezüglich der Ordnungsmässigkeit der Schlüsselverwaltung wichtige Hinweise auf die Sicherheitsmassnahmen, die eingehalten werden sollten. Im Bundesrecht werden für die Vollzugsverordnung des Bundesgesetzes über die digitale Signatur zusätzliche Bedingungen formuliert, deren Einhaltung die Revisoren prüfen sollen.

4. Im Zweifelsfall: B2B (Back-to-Basics!)

E-Business-Projekte sind komplex. Sie bergen wahrscheinlich für die Unternehmen grössere finanzielle Risiken als die Anwendungen selbst. Ihre Komplexität ruft unbedingt nach dem Aufbau eines sorgfältigen Projektrisiko-Managements.

Dieses kann beispielsweise folgende Risikokategorien umfassen:

– Risiken im Zusammenhang mit dem Projekt-Management (Personalressourcen, externe Partner, Kosten, Fristen usw.);
– Risiken im Zusammenhang mit der Durchführung des Projekts (Defini-

tion der Anforderungen, Koordination der Module, Tests, Schulung der Anwender und der Kunden usw.);
- Risiken im Zusammenhang mit der Infrastruktur und den für das Projekt ausgewählten technologischen Lösungen;
- Risiken im Zusammenhang mit dem Projektumfeld (Vereinbarkeit mit der Unternehmensarchitektur, Kollisionen mit anderen Projekten, Zusammenbruch des Marktes usw.).

Wie meistens in derart komplexen Situationen kommt auch hinzu, dass sich der Faktor Mensch ungleich folgenschwerer auswirkt als der Faktor Technologie. Die beste Verschlüsselung ist wertlos, wenn ihr Besitzer sie nicht richtig anwendet, und auch die besten firewalls können ein Unternehmen nicht schützen, das vergisst, die Berechtigung eines austretenden Angestellten zu löschen.

So weit das beruhigende Fazit aus dieser kurzen Bestandsaufnahme: Indem der Revisor überprüft, ob das Unternehmen auf qualifiziertes, in Sicherheitsfragen sensibilisiertes, fest angestelltes und motiviertes Personal zählen kann, hat er mit ziemlicher Sicherheit den wichtigsten Risiken im E-Business Rechnung getragen.

Anmerkungen

1 Information Systems Audit and Control Association, vgl. www.isaca.ch

2 Wir danken an dieser Stelle Urs Binder (Infoweek.ch), Peter Bitterli, Laurent Fabre (Ernst & Young), Monika Josi (PricewaterhouseCoopers), Patrick Ludwig (Infoguard), Christoph Protz (Arthur Andersen), Radim Svejda (Balsec) und Stéphane Vigna (KPMG).

3 International Standard on Auditing 570.

4 International Federation of Accountants.